```
     (FILE 'USPAT' ENTERED AT 15:27:37 ON 19 FEB 1999)
L1           565 S INTERCEPT### (5A) CALL#
L2          4155 S SECURITY (P) COMPONENT##
L3            14 S L1 AND L2
L4             1 S L3 AND INTERNET?
L5            76 S SECURITY? (5A) DOWNLOAD###
L6            55 S L5 AND CALL###
L7            39 S L6 AND MONITOR###
L8           363 S SANDBOX? OR ISOLAT### ENVIRONMENT##
L9             2 S L2 AND L8
L10         8911 S (SECURITY OR SAFE) (P) ENVIRONMENT##
L11          497 S L2 AND L10
L12           11 S L5 AND L11
L13          214 S L11 AND SOFTWAR###
L14          122 S L13 AND CALL#
L15           44 S L14 AND INTERCEPT###
L16           30 S L15 AND LOAD###
L17           29 S L16 AND (NETWORK OR INTERNET)
L18           17 S L17 AND DOWNLOAD###
L19           14 S L18 AND DETECT##

=> d l19 1- ti,ab
```

US PAT NO: 5,867,495 [IMAGE AVAILABLE] L19: 1 of 14
TITLE: System, method and article of manufacture for communications utilizing calling, plans in a hybrid **network**

ABSTRACT:
Telephone **calls**, data and other multimedia information is routed through a hybrid **network** which includes transfer of information across the **internet** utilizing telephony routing information and **internet** protocol address information. A media order entry captures complete user profile information for a user. This profile information is utilized by the system throughout the media experience for routing, billing, monitoring, reporting and other media control functions. Users can manage more aspects of a **network** than previously possible, and control **network** activities from a central site. Calling card access is provided for users and supports typical **calls** as well as media transfers over the hybrid **network** including over the **internet**.

US PAT NO: 5,867,494 [IMAGE AVAILABLE] L19: 2 of 14
TITLE: System, method and article of manufacture with integrated video conferencing billing in a communication system architecture

ABSTRACT:
Telephone **calls**, data and other multimedia information including video, audio and data is routed through a switched **network** which includes transfer of information across the **internet**. Users can participate in video conference **calls** in which each participant can simultaneously view the video from each other participant and hear the mixed audio from all participants. Users can also share data and documents with other video conference participants. Users can manage more

aspects of a **network** than previously possible, and control **network** activities from a central site. Billing of the conference **call** is accomplished utilizing a billing detail record to capture events associated with a **call** as they occur and debit the appropriate bill.

US PAT NO: 5,862,260 [IMAGE AVAILABLE] L19: 3 of 14
TITLE: Methods for surveying dissemination of proprietary empirical data

ABSTRACT:
An automated system checks networked computers, such as computers on the **internet**, for watermarked audio, video, or image data. A report listing the location of such audio, video or image data is generated, and provided to the proprietor(s) thereof identified by the watermark information.

US PAT NO: 5,850,481 [IMAGE AVAILABLE] L19: 4 of 14
TITLE: Steganographic system

ABSTRACT:
An identification code signal is impressed on a carrier to be identified (such as an electronic data signal or a physical medium) in a manner that permits the identification signal later to be discerned and the carrier thereby identified. The method and apparatus are characterized by robustness despite degradation of the encoded carrier, and by permeation of the identification signal throughout the carrier.

US PAT NO: 5,841,978 [IMAGE AVAILABLE] L19: 5 of 14
TITLE: **Network** linking method using steganographically embedded data objects

ABSTRACT:
A given data object can effectively contain both a graphical representation to a **network** user and embedded information, such as the URL address of another **network** node, thereby to permit the object itself to serve as an automated hot link. The underlying development tools and web site browsers create and identify such an object for use in a manner similar to a hot link, as provided on the World Wide Web.

US PAT NO: 5,832,119 [IMAGE AVAILABLE] L19: 6 of 14
TITLE: Methods for controlling systems using control signals embedded in empirical data

ABSTRACT:
An embedded multi-bit signal is steganographically **detected** from empirical data, such as image or audio data, and some aspect of a related system's operation is controlled in accordance therewith. One application of the invention is a video playback or recording device that is controlled in accordance with the embedded multi-bit signal to limit playback or recording operations. Another is a photo-duplication kiosk that recognizes certain steganographic markings in an image being copied and interrupts the copying operation.

US PAT NO: 5,822,436 [IMAGE AVAILABLE] L19: 7 of 14
TITLE: Photographic products and methods employing embedded information

ABSTRACT:
Technology is now available permitting consumers to make amateur-or even professional-grade copies of photographs. For wedding and portrait photographers, in particular, the business of making duplications is fundamental to their livelihoods. The threat of such copying is felt

strongly. To redress these concerns, a machine-readable marking is provided on emulsion films, photographic papers, and the like. The marking encodes digital information, yet is essentially imperceptible to the human eye. A photographic duplication kiosk can be constructed to read this embedded information and, if warranted by the embedded information, to disable the kiosk's copying function. An exemplary embodiment pre-exposes the photographic product with a spatial domain representation of the embedded data, and may include rotationally symmetric one-or two-dimensional patterns. Numerous other implementations are similarly practical.

US PAT NO: 5,778,368 [IMAGE AVAILABLE] L19: 8 of 14
TITLE: Real-time embedded **software** respository with attribute searching apparatus and method

ABSTRACT:
The Real-Time Embedded **Software** Repository Apparatus fully characterizes, evaluates, and reuses real-time embedded **software** that is placed or stored in a repository database. The Repository System comprises at least one Repository Client and at least one Repository Server and utilizes simulation and translational techniques to allow Real Time Embedded **Software** (RTES) to be re-used, played, and evaluated on various desktop development environments or target operating environments. The Repository System organizes and processes Repository files as Repository Units which may comprise **Software** Source Files and Test **Software**. Repository Units also contain Attachments that provide current and historic information to static files that are stored in the Repository. The Repository Units are further characterized using analysis tools (**software** analysis) which allow the user to associate fixed and user defined Attributes to the RTES. A real-time embedded component (Component) provides a clear and well defined **software** interface to function at a high level of interaction with the RTES. Templates for both searching and displaying information in a multimedia format are also provided.

US PAT NO: 5,771,354 [IMAGE AVAILABLE] L19: 9 of 14
TITLE: **Internet** online backup system provides remote storage for customers using IDs and passwords which were interactively established when signing up for backup services

ABSTRACT:
This invention makes it possible for a customer computer to connect to an online service provider computer by phone, **Internet**, or other method, pay a fee to said service provider, and obtain additional processing and storage resources for the customer's computer. The resources can take the form of virtual storage and processing capabilities. These capabilities give the customer computer what appears to be additional local processing power and/or additional local storage, this storage possibly including preloaded **software** and/or data.
The additional resources made available to the customer computer can be used either to enhance the customers' local needs (such as access to virtual storage for additional disk space, or access to a more powerful processor of similar type for program execution), or these additional resources can be used by the customer computer to support services on-line that otherwise would be unavailable, impractical, or unaffordable. Examples of services include **software** and information rental, sales, and release update services, anti-viral services, backup and recovery services, and diagnostic and repair services, to name a few.

US PAT NO: 5,748,888 [IMAGE AVAILABLE] L19: 10 of 14
TITLE: Method and apparatus for providing secure and private keyboard communications in computer systems

ABSTRACT:
A method and apparatus for providing secure and private keyboard communications in a computer system. A request for private keyboard communications causes the computer's processor to enter into system management mode by generating an system management interrupt. A secure system management interrupt handler then directs specialized hardware to **intercept** and divert keyboard interrupts, such that data entered via the keyboard is only communicated to a non-readable black box security device that controls access to protected system resources. Keyboard data is thereby protected from **interception** by malicious **software**.

US PAT NO: 5,748,783 [IMAGE AVAILABLE] L19: 11 of 14
TITLE: Method and apparatus for robust information coding

ABSTRACT:
A digital signal is imperceptibly embedded into an input source signal, such as an image or video signal, to produce an encoded (sometimes termed "watermarked") signal. The principle of quasi-rotational symmetry is employed to facilitate detection of the embedded signal notwithstanding rotation of the encoded signal. Single or multiple degrees of symmetry can be employed. In another aspect, the digital signal is transformed to a frequency domain and phase-only filtered prior to its combination with the input source signal. In an illustrative embodiment, this filtering operation helps hide the digital signal within the source signal, and facilitates detection of the embedded digital signal even after the encoded signal has undergone various forms of corruption.

US PAT NO: 5,748,763 [IMAGE AVAILABLE] L19: 12 of 14
TITLE: Image steganography system featuring perceptually adaptive and globally scalable signal embedding

ABSTRACT:
An identification code signal is hidden in a carrier signal (such as an electronic data signal or a physical medium) in a manner that permits the identification signal later to be discerned. The carrier signal can thereby be identified, or some machine responsive action can thereby be taken. In one image steganography embodiment, the relative strength of the identification code signal is both perceptually adapted in accordance with psychovisual characteristics of the image, and globally scaled in accordance with a user-set visibility control. The technique can be applied in video imagery embodiments to control associated video equipment, e.g. to serve as a copy control signal.

US PAT NO: 5,710,834 [IMAGE AVAILABLE] L19: 13 of 14
TITLE: Method and apparatus responsive to a code signal conveyed through a graphic image

ABSTRACT:
An identification code signal is impressed on a carrier to be identified (such as an electronic data signal or a physical medium) in a manner that permits the identification signal later to be discerned and the carrier thereby identified. The method and apparatus are characterized by robustness despite degradation of the encoded carrier, and by permeation of the identification signal throughout the carrier.

US PAT NO: 5,636,292 [IMAGE AVAILABLE] L19: 14 of 14
TITLE: Steganography methods employing embedded calibration data

ABSTRACT:
An identification code signal is impressed on a carrier to be identified (such as an electronic data signal or a physical medium) in a manner that permits the identification signal later to be discerned and the carrier

thereby identified. The method and apparatus are characterized by robustness despite degradation of the encoded carrier, and by permeation of the identification signal throughout the carrier.

intercept### (5a) call# 704, 186 184.01

08/825102 APS

(FILE 'USPAT' ENTERED AT 13:24:19 ON 19 FEB 1999)
L1 28432 S ~~395~~/?/CCLS ~~714—709~~
L2 2285 S INTERCEPT### (P) LOAD?
L3 131 S L1 AND L2
L4 29 S L3 AND SECURITY?
L5 28 S L4 AND CALL?
L6 14 S L5 AND (SOFTWARE# (P) COMPONENT#)

=> d l6 1- ti,ab

US PAT NO: 5,842,011 [IMAGE AVAILABLE] L6: 1 of 14
TITLE: Generic remote boot for networked workstations by creating local bootable code image

ABSTRACT:
A system and method for booting a client workstation from a remote data processing system over a network includes initializing the client workstation sufficiently to establish network communications with a remote disk on the remote data processing system, establishing a network communications link between the local and remote systems, issuing a request from the client workstation to the remote data processing system over the network communications link for a task image code module for providing a network interface between the client workstation and the remote disk on the remote data processing system, downloading the task image code module from the remote to the client workstation in response to the request for the task image code module, invoking the task image code module by the client workstation to establish a network interface between the client workstation and the remote disk, copying an image of the remote disk over the network to the client workstation to create a local disk image stored in the client workstation, disconnecting the client workstation from the network, booting the client workstation from the disk image stored in the client workstation, including loading an operating system module from the disk image into the client workstation, invoking the operating system module to control the client workstation, loading network environment modules from the disk image into the client workstation under control of the operating system module, and invoking the network environment modules to establish a network communication link between the client workstation and the remote data processing system.

US PAT NO: 5,841,978 [IMAGE AVAILABLE] L6: 2 of 14
TITLE: Network linking method using steganographically embedded data objects

ABSTRACT:
A given data object can effectively contain both a graphical representation to a network user and embedded information, such as the URL address of another network node, thereby to permit the object itself to serve as an automated hot link. The underlying development tools and web site browsers create and identify such an object for use in a manner similar to a hot link, as provided on the World Wide Web.

US PAT NO: 5,835,722 [IMAGE AVAILABLE] L6: 3 of 14
TITLE: System to control content and prohibit certain interactive attempts by a person using a personal computer

User Name: NNguyen2

User Phone: 0003053900

Workstation Id: ws05077

Printer Id: \USPTO-FP-01GBGHPTR GPPTR PK2-2B01

Date: Thu Feb 18, 1999

Time: 13:13:58

NT Job

Documents Requested

(01) 05872942 U (02) 05812800 U (03) 05809261 U
(04) 05784650 U

Sections Requested

Front Page, Drawings, Specifications, Claims, Changes/Corrections, Reexaminations

ABSTRACT:
A computer terminal and a method for blocking the use and transmission of vulgar and pornographic material in a responsive and interactive manner that comprehensively monitors computer operations for creation or transmission of vulgar and pornographic material. Data created by the keyboard, data passing through the clipboard, data selected by the mouse pointer, and data passing through the Internet interface are monitored for content and further operation of the computer terminal is blocked. The computer terminal may only be unblocked by a supervisory intervention, such as by entering of a password, or by restarting or resetting the terminal. Key word searches, such as those in Internet search engines, are also monitored, but the terminal adapts to monitor not only for words of a profane and vulgar nature, but also for words that are behaviorally tested to produce lists containing vulgar and profane items, e.g., Internet sites. The computer terminal and method can be modified to block other forms of communication or computer operation, such as blocking transmission of secret business data, blocking execution or opening of certain programs or files, and the like.

US PAT NO: 5,809,230 [IMAGE AVAILABLE] L6: 4 of 14
TITLE: System and method for controlling access to personal computer system resources

ABSTRACT:
A system and method for controlling access to computer resources of a computer is disclosed. The access control program preferably includes a plurality of program components, which may be terminate stay resident (TSR) programs, for intercepting interrupt service **calls**. The interrupt service **calls** are verified to determine whether the user is authorized for the resource requested in the service **call**. The program components use files containing a list of authorized resources for the computer user. These files are, preferably, used at system initialization to modify the system resource files used by the operating system to identify program and program groups which are displayed to a user. A boot protection program is also disclosed which may be installed with the access control program to prevent a boot program stored on media within the diskette drive from acquiring control of the system during system initialization. The boot protection program corrupts the master boot record, boot record and partition table so that other boot programs do not have sufficient information to initialize the system. The master boot program is modified to access this requisite information elsewhere during system initialization.

US PAT NO: 5,771,354 [IMAGE AVAILABLE] L6: 5 of 14
TITLE: Internet online backup system provides remote storage for customers using IDs and passwords which were interactively established when signing up for backup services

ABSTRACT:
This invention makes it possible for a customer computer to connect to an online service provider computer by phone, Internet, or other method, pay a fee to said service provider, and obtain additional processing and storage resources for the customer's computer. The resources can take the form of virtual storage and processing capabilities. These capabilities give the customer computer what appears to be additional local processing power and/or additional local storage, this storage possibly including preloaded software and/or data.
The additional resources made available to the customer computer can be used either to enhance the customers' local needs (such as access to virtual storage for additional disk space, or access to a more powerful processor of similar type for program execution), or these additional

User Name: NNguyen2

User Phone: 0003053900

Workstation Id: ws05077

Printer Id: \USPTO-FP-01GBGHPTR GPPTR PK2-2B01

Date: Thu Feb 18, 1999

Time: 13:16:24

NT Job

Patent ID	Document Not Available	Pages Not Available	150 dpi Pages	Unscanned Pages	Total Pages Printed
05872942	000	000	000	000	044
05812800	000	000	000	000	018
05809261	000	000	000	000	042
05784650	000	000	000	000	016

resources can be used by the customer computer to support services on-line that otherwise would be unavailable, impractical, or unaffordable. Examples of services include software and information rental, sales, and release update services, anti-viral services, backup and recovery services, and diagnostic and repair services, to name a few.

US PAT NO: 5,748,888 [IMAGE AVAILABLE] L6: 6 of 14
TITLE: Method and apparatus for providing secure and private keyboard communications in computer systems

ABSTRACT:
A method and apparatus for providing secure and private keyboard communications in a computer system. A request for private keyboard communications causes the computer's processor to enter into system management mode by generating an system management interrupt. A secure system management interrupt handler then directs specialized hardware to intercept and divert keyboard interrupts, such that data entered via the keyboard is only communicated to a non-readable black box **security** device that controls access to protected system resources. Keyboard data is thereby protected from interception by malicious software.

US PAT NO: 5,737,416 [IMAGE AVAILABLE] L6: 7 of 14
TITLE: Method and apparatus for enabling trial period use of software products: method and apparatus for utilizing a decryption stub

ABSTRACT:
A method and apparatus is provided in a data processing system for securing access to particular files which are stored in a computer-accessible memory media. A file management program is provided as an operating system component of the data processing system. At least one encrypted file and at least one unencrypted file are stored in the computer-accessible memory media. An unencrypted **security** stub is associated with each of the encrypted files. The **security** stub is at least partially composed of executable code. The file management program is utilized to monitor data processing **calls** for a **called** file stored in the computer-accessible memory media. The file management program determines what the **called** file has an associated unencrypted **security** stub. The **called** file is processed in a particular manner dependent upon whether or not the **called** file has an associated unencrypted **security** stub.

US PAT NO: 5,689,560 [IMAGE AVAILABLE] L6: 8 of 14
TITLE: Method and apparatus for enabling trial period use of software products: method and apparatus for allowing a try-and-buy user interaction

ABSTRACT:
A method and apparatus is provided for distributing software objects from a producer to a potential user. The software object is reversibly functionally limited, preferably through encryption, and loaded onto a computer-accessible memory media along with the file management program. The computer-accessible memory media is shipped from the producer to the potential user. The file management program is loaded into a user-controlled data processing system, and associated with the operating system for the user-controlled data processing system. The computer-accessible memory media is read with the user-controlled data processing system. The file management program is utilized to restrict access to the software object.

US PAT NO: 5,608,865 [IMAGE AVAILABLE] L6: 9 of 14
TITLE: Stand-in Computer file server providing fast recovery from computer file server failures

User Name: NNN

User Phone:

Workstation Id: GPRBURGI

Printer Id: gbgiptr

Date: Thu Feb 18, 1999

Time: 07:19:19

Job # 11085

Patent ID	Document Not Available	Pages Not Available	150 dpi Pages	Unscanned Pages	Total Pages Printed
05870087	000	000	000	000	027
05864607	000	000	000	000	038
05850436	000	000	000	000	038

Filtering Started: Thu Feb 18 07:18:43 1999
Retrieval Started: Thu Feb 18 07:18:44 1999
Filtering Finished: Thu Feb 18 07:19:05 1999
Printing Started: Thu Feb 18 07:19:19 1999

ABSTRACT:
An Integrity Server computer for economically protecting the data of a computer network's servers, and providing hot standby access to up-to-date copies of the data of a failed server. As the servers' files are created or modified, they are copied to the Integrity Server. When one of the servers fails, the Integrity Server fills in for the failed server, transparently providing the file service of the failed server to network clients. The invention provides novel methods for managing the data stored on the Integrity Server, so that the standby files are stored on low-cost media such as tape, but are quickly copied to disk when a protected server fails. The invention also provides methods for re-establishing connections between clients and servers, and communicating packets between network nodes, to allow the Integrity Server to stand-in for a failed server without requiring reconfiguration of the network clients.

US PAT NO: 5,491,808 [IMAGE AVAILABLE] L6: 10 of 14
TITLE: Method for tracking memory allocation in network file server

ABSTRACT:
A method for dynamically tracking memory resource allocations/deallocations of a program resident in the memory of a network file server is disclosed wherein **calls** to system memory allocation functions are intercepted and diverted to memory resident tracker routines, interposed between the **caller** and the **called** functions to monitor returns from the **called** functions. Public symbol lists of application program interfaces are scanned for functions to be tracked, and function entry points are taken over by replacing initial instructions of the system functions with jumps to the tracker routines. The tracker routines then **call** the remainder of the system functions and record the reply before passing control back to the original **caller** program. Information on allocated blocks is written to ABLK blocks taken from an ABLK free block pool allocated at tracker startup. Subsequent deallocations of the allocated blocks release the same ABLK blocks back to the ABLK free pool. Information on "NULL" pointer and similar returns indicating allocation/deallocation errors is written to MSG queue blocks taken from a MSG free block pool allocated at tracker startup. Log file generator threads are activated to list the filled ABLK and MSG blocks when signalled. Cleanup routines restore the replaced code and deallocate all ABLK and MSG memory blocks when the tracker exits.

US PAT NO: 5,452,454 [IMAGE AVAILABLE] L6: 11 of 14
TITLE: Generic remote boot for networked workstations by creating local bootable code image

ABSTRACT:
A system and method for booting a client workstation from a remote data processing system over a network includes initializing the client workstation sufficiently to establish network communications with a remote disk on the remote data processing system, establishing a network communications link between the local and remote systems, issuing a request from the client workstation to the remote data processing system over the network communications link for a task image code module for providing a network interface between the client workstation and the remote disk on the remote data processing system, downloading the task image code module from the remote to the client workstation in response to the request for the task image code module, invoking the task image code module by the client workstation to establish a network interface between the client workstation and the remote disk, copying an image of the remote disk over the network to the client workstation to create a local disk image stored in the client workstation, disconnecting the

client workstation from the network, booting the client workstation from the disk image stored in the client workstation, including loading an operating system module from the disk image into the client workstation, invoking the operating system module to control the client workstation, loading network environment modules from the disk image into the client workstation under control of the operating system module, and invoking the network environment modules to establish a network communication link between the client workstation and the remote data processing system.

US PAT NO: 5,392,400 [IMAGE AVAILABLE] L6: 12 of 14
TITLE: Collaborative computing system using pseudo server process to allow input from different server processes individually and sequence number map for maintaining received data sequence

ABSTRACT:
A collaborative computing method and system are described. Output data from and input data for an application program are shared among all of the computers connected in a network using the X protocol. The output from the application program is intercepted and then replicated on each of the computers' displays. Input data for the application program can be read from any of the computers participating in the session. The identifying data associated with the output and input is modified so that each computer can operate as if it were the only computer controlling the application. The session is controlled by displaying on each computer's display a control window which allows the users to invoke a shared application and to use tools such a pointer, marker, to manage a collaboration session. Each user has equal collaborative capabilities in a session. This collaborative method provides a symmetric sharing among all users. A scratch pad window may be created on each computer's display. User data entered in a scratch pad window is normally replicated automatically on each of the other computers' displays, but a private mode is an alternative. Data entered by each computer in the scratch pad may be displayed with visual characteristics such as color which are unique to the computer on which the data was first entered.

US PAT NO: 4,935,870 [IMAGE AVAILABLE] L6: 13 of 14
TITLE: Apparatus for downloading macro programs and executing a downloaded macro program responding to activation of a single key

ABSTRACT:
Apparatus for downloading videotex information via a host computer includes a group of local terminals installed at a variety of locations. The terminals receive and store macro programs from the host computer. The local terminal then activates the macro programs via a set of function input devices, which generate macro program activating signals.

US PAT NO: 4,591,967 [IMAGE AVAILABLE] L6: 14 of 14
TITLE: Distributed drum emulating programmable controller system

ABSTRACT:
Master units and slave units are preferably housed in identical housings. Each master unit comprises a Central Intelligence Unit (CIU) which in turn comprises a drum processor and a communications processor, and an Input/Output Unit (IOU) having input terminals and relays for connection to external devices. Each slave unit comprises an IOU. Each IOU is connected to its CIU through a Local bus (L-bus). Up to sixteen IOU's may be controlled by a single CIU.
Up to 16 master units may be connected together by means of console bus (C-bus) and a data exchange bus (X-bus), in which case each master unit is given control of specified "X" variables for update. Each "X" variable has a specific time slot on the X-bus and all "X" variables are stored on

an X-drum at each master unit.
The C-bus may be connected to a computer terminal at each master for programming of all CIU's, or to computer devices, or to long distance communication lines.
Each IOU monitors continuously 32 identical input ports and maintains in a table the voltage at that port, whether the voltage has gone up or down through preselected voltages and the number of times this has happened since the last interrogation by its CIU on the L-bus. These tables are transmitted upon interrogation to its CIU. The program at the master can therefore interpret each input as a voltage, a switch, or a pulse source. Each IOU employs a digital filter in its program for interpreting the voltage of the inputs.